Senate Study Bill 3183

SENATE FILE _____
BY (PROPOSED COMMITTEE ON COMMERCE BILL BY CHAIRPERSON WARNSTADT)

Passed Senate, Date _____ Passed House, Date _____
Vote: Ayes _____ Nays _____ Vote: Ayes _____ Nays _____
Approved _____

A BILL FOR

An Act relating to identity theft, including providing for the notification of a breach in the security of computerized data that includes personal information, establishing a business duty to safeguard personal information against a breach of security, and providing penalties.
BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:
TLSB 5657XC 82
rn/nh/8

PAG LIN

Section 1. NEW SECTION. 715C.1 DEFINITIONS.
As used in this chapter, unless the context otherwise requires:
1. "Breach of security" means unauthorized acquisition of computerized data maintained by a person that materially compromises the security, confidentiality, or integrity of personal information maintained by the person. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
2. "Consumer" means an individual who is a resident of this state.
3. "Consumer reporting agency" means the same as defined by the federal Fair Credit Reporting Act, 15 U.S.C. } 1681a.
4. "Debt" means the same as provided in section 537.7102.
5. "Encryption" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.
6 "Extension of credit" means the right to defer payment of debt or to incur debt and defer its payment offered or granted primarily for personal, family, or household purposes.
7. "Financial institution" means the same as defined in section 536C.2, subsection 6.
8. "Identity theft" means the same as provided in section 715A.8.
9. "Payment card" means the same as defined in section 715A.10, subsection 3, paragraph "b".
10. "Person" means an individual; corporation; business trust; estate; trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity.
11. "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if neither the name nor the data elements are encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:
a. Social security number.
b. Driver's license number or other unique identification number created or collected by a government body.
c. Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

d. Unique electronic identifier or routing code, in combination with any required security code, access code, or password.

12. "Redacted" means altered or truncated so that no more than the last four digits of a social security number or other numbers designated in section 715A.8, subsection 1, paragraph "a", is accessible as part of the data.

Sec. 2. NEW SECTION. 715C.2 SECURITY BREACH == CONSUMER NOTIFICATION == REMEDIES.

1. Any person who owns, maintains, or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and who was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification under subsection 2, to any consumer whose personal information was included in the information that was breached. The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection 3, and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

2. Any person who maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer's personal information was included in the information that was breached.

3. The consumer notification requirements of this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the person required to give notice in writing.

4. For purposes of this section, notification to the consumer may be provided by one of the following methods:

a. Written notice.

b. Electronic notice if the person's customary method of communication with the consumer is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in chapter 554D and the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. } 7001.

c. Telephone notice, provided that the contact is made directly with the affected consumer.

d. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, that the affected class of consumers to be notified exceeds three hundred fifty thousand persons, or if the person does not have sufficient contact information to provide notice. Substitute notice shall consist of the following:

(1) Electronic mail notice when the person has an electronic mail address for the affected consumers.

(2) Conspicuous posting of the notice or a link to the notice on the internet web site of the person if the person maintains an internet web site.

(3) Notification to major statewide media.

5. Notice pursuant to this section shall include, at a minimum, all of the following:

a. A description of the breach of security.

b. The approximate date of the breach of security.

c. The type of personal information obtained as a result of the breach of security.

d. Contact information for consumer reporting agencies.

e. Advice to the consumer to report suspected incidents of identity theft to law enforcement, including the federal trade commission.

6. Notwithstanding subsection 1, notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be

maintained for five years.
7. This section does not apply to any of the following:
a. A person who complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator.
b. A person who complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section.
c. A person who is subject to and complies with regulations promulgated pursuant to Title V of the Gramm=Leach=Bliley Act of 1999, 15 U.S.C. } 6801==6809.
8. a. The attorney general may take appropriate action to enact this chapter or bring an action on behalf of an injured person for an injunction, actual damages incurred by the person, attorney fees, interest, and court costs.
b. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law.
Sec. 3. NEW SECTION. 715C.3 PERSONAL INFORMATION == BUSINESS DUTY TO SAFEGUARD == RIGHT OF ACTION == DAMAGES AND PENALTIES.
1. Any person who accepts a payment card in connection with transactions occurring in the ordinary course of business has a duty to comply with or adhere to payment card industry data security standards. A financial institution may bring an action against a person who is subject to a breach of security if the person is found at the time of the breach to have engaged in or violated such data security standards.
2. In an action commenced by a financial institution to recover damages pursuant to subsection 1, the financial institution shall submit in writing a request that the person alleged to have violated this section certify compliance with the standards pursuant to a payment card industry=approved independent auditor or another person authorized to issue such a certification. A presumption of compliance shall exist if a person contracts for or utilizes the services of a third party to collect, maintain, or store personal information used in connection with a payment card, and contractually requires that the third party ensure compliance with the standards on an ongoing basis.
3. a. A financial institution prevailing in an action for failure to safeguard personal information against a breach of security may recover actual damages arising from the failure. Actual damages shall include any costs incurred by the financial institution in relation to the following:
(1) Cancellation or reissuance of a payment card affected by the security breach.
(2) Closing of a deposit, transaction, share draft, or other account affected by the security breach and any action to stop payment or block a transaction with respect to the account.
(3) Opening or reopening of a deposit, transaction, share draft, or other account affected by the security breach.
(4) Refunding or crediting made to an account holder to cover the cost of any unauthorized transaction relating to the breach of security.
(5) Notification to account holders affected by the breach of security.
b. Reasonable attorney fees and costs shall be awarded to the prevailing party, with the exception that an award shall not be made to a person who failed to submit certification as required in subsection 2.
c. An action pursuant to this section shall not be commenced against any person other than a person who has been found to have violated this section.
4. The attorney general may adopt rules necessary to implement this section, which may include identification of payment card industry standards to be applied.

EXPLANATION

This bill provides for the notification of a breach in the security of computerized data of personal information, and establishes a business duty to safeguard such information against security breaches.
The bill requires a person who owns, maintains, or otherwise possesses computerized data that includes personal

information to provide notice of any breach of the person's security of the data to those residents of this state whose personal information was or may have been acquired by an unauthorized person. The bill also requires a person who maintains computerized data that includes personal information that the person does not own to notify the owner of the data of any breach in the security of the data. A "person" is defined in the bill to include persons that conduct business in this state and state agencies. The notice shall be provided immediately unless a law enforcement agency determines that the notification will impede a criminal investigation. The notice may be made in writing, through electronic means, or by substitute notice, as defined in the bill, and must contain information regarding a description of the breach of security, the approximate date of the breach, the type of personal information obtained, contact information for consumer reporting agencies, and consumer reporting advice.

The bill provides that notification will not be required if an investigation or consultation with law enforcement agencies determines that no reasonable likelihood of harm has or will result from the breach, and that the bill's provisions do not apply to persons complying with specified requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements as provided pursuant to the bill.

The bill provides that the attorney general may bring a civil action on behalf of an injured person.

The bill additionally establishes a duty with respect to a person who accepts a payment card in connection with business transactions to adhere to payment card industry data security standards. The bill authorizes a financial institution, as defined in the bill by reference to include a bank, savings and loan association, or credit union organized under the provisions of any state or federal law, and their affiliates, to bring an action against a person who is subject to a breach of security if the person is found at the time of the breach to have engaged in or violated such data security standards.

The bill requires a financial institution to submit a written request that a person alleged to have failed to protect personal information certify compliance with the standards pursuant to a payment card industry=approved independent auditor or another person authorized to issue such a certification. A presumption in favor of compliance exists if a person contracts for or utilizes the services of a third party to collect, maintain, or store personal information used in connection with a payment card, and requires that the third party ensure compliance with the standards on an ongoing basis.

Actual damages which may be recovered by a financial institution can include any costs incurred by the financial institution relating to cancellation or reissuance of a payment card; closing of a deposit, transaction, share draft, or other account affected and any action to stop payment or block a transaction; opening or reopening of a deposit, transaction, share draft, or other account; refunding or crediting made to an account holder to cover the cost of any unauthorized transaction; and notification to account holders affected by the breach of security. The bill also awards attorney fees and costs to a prevailing party unless that party is a person who failed to comply with the written certification request. Further, the bill provides that an action for failure to adhere to date security standards cannot be commenced against any person other than a person who has been found to have violated such standards, other than an award of attorney fees and costs if the financial institution is not a prevailing party.

The bill provides that the attorney general shall adopt rules necessary to implement the bill's provisions, including identification of payment card industry standards to be applied.

LSB 5657XC 82
rn/nh/8